Electronic Mail Server Security Standard

Scope: The standard applies to all state agencies, departments, institutions, commissions, committees, boards, divisions, bureaus, offices, officers, and officials of the State as set out in Article 147, Article 3D.

1.0 Rationale[1]

To reduce unauthorized access to electronic mail (e-mail) systems by requiring security measures that are commensurate with the risks attendant to such systems.

2.0 Enterprise Wide Standard

All e-mail services offered or subscribed to by state agencies subject to G.S. §147-33.110 must adhere to the security requirements of this standard.[2]

2.1 Configuration

1. All services and operations shall be disabled except those which are expressly permitted (*e.g.,* Web based mail, FTP, remote administration) and only the minimal Internet services required shall be installed.

2. Default accounts and groups shall be disabled or removed.

3. The service banner shall not report the mail server and operating system type and version.

4. The mail server shall be configured to use encrypted authentication of passwords or other authentication data.

.

5. All mail servers used to relay mail, e.g., via the SMTP protocol from email client software, shall be configured to only accept email from authenticated sources.[3]

6. All servers used to receive email, e.g., from external sources via the SMTP protocol, shall be configured to only accept incoming mail for email domains they represent.

7. All mail servers where possible shall not allow the "from," or alternative standard return header, to be an email address domain that it does not represent

8. All mail servers used to relay mail shall be configured to rate limit message delivery to within acceptable performance standards to reduce successful Denial of Service (DoS) attacks.

---

[1] This standard is primarily based upon principles set forth in NIST Special Publication 800-45, Version 2 (2007) "Guidelines on Electronic Mail Security".

[2] E-mail services also must comply with other security standards and policies, including the User ID and Password Protection Standard and Virus Protection Policy with Guidelines.

[3] This can be achieved by login credentials sent over an encrypted connection or by connection from specific IPs before the server accepts the mail to be sent.

9. Any mail transport agent (MTA) server software used solely for the purpose of allowing a local application to send emails, e.g., monitoring software that sends alerts via SMTP, shall be installed and configured so that:

    - Its only function is to send, not receive email.
    - It can only send to the host(s) whose function(s) is(are) the primary mail server for the agency.
    - It accepts connections only from the host it is installed on, eg., via localhost or socket.
    - It has a valid sending email address that can accept bounces if any.
    - Where possible, the server shall not allow the "From" or alternative standard header to be an email address domain that it does not represent.

2.2 Mail Server

A mail server shall be on a dedicated, single-purpose host, whether it is a physical server or a virtualized server. The server shall have a dedicated physical disk or logical partition for mailboxes (separate from the operating system and server application).

All mail commands which can be used to obtain information on accounts, or are otherwise unnecessary or dangerous, that are not required for normal operation (*e.g.,* VRFY and EXPN) shall be disabled.

All mail servers shall use a file integrity checker to monitor changes to critical files on the mail server (host-based or file-integrity checker)[4]

2.3 Firewall/Mail Relay

1. The mail server shall be protected by a firewall that controls all traffic between the Internet and the server.
2. Incoming and outgoing messages shall be scanned for viruses at the firewall or mail relay. If attachments are allowed on the e-mail service, the mail server administrator shall filter potentially dangerous attachment types (*e.g.*, .exe, .vbs, .ws, .wsc file extensions) at the mail server or mail gateway and conduct virus scans on allowed file types.
3. The firewall (or router that is acting as a firewall) shall block all access to the mail server from the Internet except those ports that are required to operate the e-mail server.
4. Where possible, the server containing the mailboxes shall be located in a secure zone separate from the server(s) whose function is to send/receive email, authenticates end users, and/or provides web-based access.

2.4 Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

1. IDS/IPS shall monitor network traffic to and from the mail server.

---

[4] Some critical files will change regularly and, therefore, should not be protected by a file integrity checker. The determination of which files should be protected will depend on the mail server and the operating system used.

2. A firewall, in conjunction with IDS/IPS, shall block IP addresses or subnets that the IDS/IPS reports are attacking the organizational network.

3. IDS/IPS shall be configured to log events and the logs shall be maintained for at least three months. The retention of logs must also comply with any relevant legal and regulatory requirements, including the agency's records retention schedule.

4. IDS/IPS monitoring the mail server shall be updated with new attack signatures at least weekly.

2.5 Physical Security

E-mail servers and related items such as communication wiring and networks shall be located in secure locations that are locked and restricted to access by authorized personnel only.

GUIDELINE

When evaluating upgrades to e-mail servers, the inclusion of technology allowing electronic signatures for signing messages for sender validation should be considered.

November 7, 2008: Approved as amended by the State CIO